## COMMENTS

The enclosed is responsive to Examiner's Office Action mailed on July 25, 2007. At the time Examiner mailed the Office Action claims 20-36 and 67-82 were pending. By way of the present response Applicant has amended claims 29, 67, 71, and 79, cancelled claims 20-28 and added no new claims. As such, claims 29-36 and 67-82 are now pending. Applicants respectfully request reconsideration of the present application and the allowance of all claims now presented. No new matter has been added.

## INTERVIEW SUMMARY

Applicants thank the Examiner for the telephonic interview conducted on 10/19/2007, at which claim 67 was discussed in relation to references U.S. 7,007,068 B2 ("Morkel") and Ben Livingston (ben@drizzlesSPAM.com; Possible modifications to Washington, anti-spam law, Internet Newsgroup, January 31, 2002) ("Livingston"), cited by the Examiner in the Office Action mailed 7/25/2007. No agreement was reached.

## Claim Rejections – 35 USC §103

Claims 20-36 and 67-79 are rejected under 35 U.S.C. 103(a) as being unpatentable over Morkel, U.S. 7007068 B2 (hereinafter "Morkel") in view of Ben Livingston (ben@drizzlesSPAM.com; Possible modifications to Washington, anti-spam law, Internet Newsgroup, January 31, 2002).

No Suggestion or Motivation to Combine References

Applicant respectfully submits that there is no suggestion or motivation to make the proposed combination as the proposed combination of Morkel and Livingston renders the prior art unsatisfactory for its intended purpose (See MPEP § 2143.01(V)).

Morkel describes a system that allows an email sender to control the time and frequency of sending updates of personal information (contact information) to select recipients and to securely protect the access of personal information so that the personal information is received only by the selected recipients (Col 2, lines 4-10). To securely protect the personal information, either the recipient's email address or the user's email address is hashed, depending on the particular embodiment (Col 2, lines 22-26, 37-39, 51-53). That hashed email address is compared with either a stored hash on a server or with another computed hash of the email address. If the hashes match, the server will transmit the personal information to the recipient (Col 2, lines 43-46, 54-58). Thus in this fashion, the personal information of the sender will be securely transmitted to the recipient.

Livingston describes a "do not email" list where a "spammer must contact the domain name registrant for every email address on their list" so as to exclude recipients from a mailing list (Paragraph 3). Livingston also states "I feel that a 'do not email' list would work well' **unfortunately, such a list could be seriously abused**" (Paragraph 4, emphasis added).

The proposed combination of Morkel and Livingston would have the "do not email" list of Livingston incorporated into the secure transmission of personal contact information of Morkel. However, this proposed combination would render the prior art reference of Morkel unsatisfactory for its intended purpose. Placing the hashed email address (either sender or recipient) on a "do not email" list would defeat the purpose of Morkel. As previously described, the intended purpose of Morkel is for the secure transmission of personal contact information. Reception of the email message is vital; personal contact information cannot be exchanged in the system of Morkel if the email address is placed on a "do not email" list. In other words, personal contact information cannot be exchanged via the Morkel email system if the recipient's email is blocked by a "do not email" list. Thus, there is no motivation or suggestion to combine Morkel and Livingston. Therefore, the proposed combination does not describe the limitations in claims 20-36 and 67-79.

For at least these reasons, Applicant respectfully submits that the independent claims 29, 67, 71, and 79 are allowable. Applicant respectfully submits that the dependant claims 30-36, 68-70, 72-78, and 80-82 are allowable for at least the reason that they are dependent on an allowable independent claim.

Claims 80-82 are rejected under 35 U.S.C. 103(a) as being unpatentable over Morkel in view of Ben Livingston further in view of Lu (US 7174453 B2).

Applicant respectfully submits that the dependent claims 80-82 are allowable for at least the reason they are dependent on an allowable independent claim 79, which is discussed above.

Combination does not describe required claim limitations

Applicant respectfully submits that even if Morkel and Livingston can be properly combined, the proposed combination does not describe the required claim limitations.

Claim 29

Claim 29 as amended requires (emphasis added):

> collecting a set of one or more do-not-email list entries, each do-not-email list entry is a string of characters representing an email address;
> applying a one-way hashing scheme to the set of one or more do-not-email list entries to convert the strings of characters into unique hashed values to create a set of one or more hashed do-not-email list entries, wherein the one-way hashing scheme is intended to conceal the do-not-email list entries from an intended recipient;
> transferring the set of one or more hashed do-not-email list entries to a master do-not-email list server configured to store the set of one or more hashed do-not-email list entries without revealing the email address corresponding to each of the hashed do-not-email list entries;
> requesting from the master do-not-email list server at least one hashed do-not-email list entry from the set of one or more hashed do-not email list entries to create or update a client do-not-email list on a client machine;
> causing a client email entry to be hashed using the same one-way hashing scheme to create a hashed client email entry;
> comparing the hashed client email entry to the hashed do-not-email list entries on the client do-not-email list to determine whether the hashed client email entry appears on the client do-not-email list; and
> transmitting at least one email to the email address that corresponds to the hashed client email entry upon determining that the hashed client email entry does not appear on the client do-not-email list.

Applicant respectfully submits that the combination of Morkel and Livingston does not describe the limitations as required in amended claim 29. The proposed combination of Morkel and Livingston would have the "do not email" list of Livingston incorporated into the secure transmission of personal

contact information of Morkel. However, as previously described, Morkel uses hashing to confirm the identity of the parties, and once the identity is confirmed, unhashed data (personal contact information) will be shared. Personal contact information includes an email address (Col 1, lines 30-35). Thus, Morkel shares the underlying email address. Applicant's claimed invention, however, requires comparing a "hashed client email entry to the hashed do-not-email list entries on the client do-not-email list to determine whether the hashed client email entry appears on the client do-not-email list; and transmitting at least one email to the email address that corresponds to the hashed client email entry upon determining that the hashed client email entry does not appear on the client do-not-email list" (amended claim 29).

As recognized by Livingston ("a do-not email list would well; unfortunately, such list could be seriously abused", Paragraph 4), by way of example and not limitation, Applicant's claimed invention allows a client email marketer the ability to identify email addresses on a do-not-contact list that are in the client's list without revealing the unhashed email addresses on the do-not-contact list or the client's list. Thus, by way of example and not limitation, Applicant's claimed invention prevents the abuse of the do-not-email list that is recognized by Livingston.

To illustrate, an email marketer has one list of email addresses that the email marketer wants to contact for marketing purposes and another party, in our example the government, has their own list of email addresses that make up a do-not-contact list. The email marketer is not allowed to contact email

addresses that choose to opt out of email marketing (i.e., the email addresses on the government's list) so the email marketer desires to check the entries on the government's list to determine if the email marketer should remove an entry from their list.

However, the government does not want to share their list of unhashed email addresses that do not wish to be contacted as this information can be very valuable to unscrupulous email marketers (e.g., if the list of unhashed email addresses were compromised then unscrupulous email marketers could contact the email addresses of people that do not wish to be contacted). Additionally, the email marketer also does not want to share their list of unhashed email addresses because this information is also very valuable to the email marketer and they do not want this list to be public for fear of unscrupulous email marketers (e.g., for the same reasons as above). Therefore, in Applicants' claimed invention a one-way hashing scheme is used by both entities (government and email marketer) such that each entity will have a list containing hashed entries. These two lists can then be compared and matches determined. Thus, with Applicants' claimed invention, for example, the content of the lists (i.e., the email addresses that on both lists) can be compared (e.g., by comparing the hashed entries on both lists) in order to modify the email marketer's list by removing the email addresses that appear on the government's do not email list without sharing the lists of unhashed email addresses. The email marketer may then transmit email messages to the email addresses that are not on their list that are not on the governments list.

Applicant respectfully submits that the dependant claims 30-36 depend on amended claim 29 and are allowable for at least the same reason.

Claim 67

Claim 67 as amended requires (emphasis added):

> A computer implemented method to identify email addresses registered on a do not contact list that are in a client's list without revealing the email addresses on the do not contact list or the client's list comprising:
>
> the client encrypting at least certain of entries on the client's list to create a plurality of encrypted entries, where each entry includes at least an email address, wherein the entries are encrypted in a way that it is intended that an intended recipient cannot decrypt the entries;
>
> the client transmitting over a network said plurality of encrypted entries from the client's list to a service for comparison to encrypted entries of the do not contact list, wherein the encrypted entries of the do not contact list were formed by encrypting information, including at least an email address, a matching of an encrypted entry from said plurality of encrypted entries from the client's list to an entry of the do-not-contact list represents that the underlying email address needs to be identified;
>
> the client receiving results of the comparison, wherein the results of the comparison are an indication of which encrypted entries on the client's list match the encrypted entries on the do not contact list, and the results are not unencrypted entries of the do not contact list; and
>
> the client transmitting at least an email to the email addresses in the client's list that correspond to the encrypted entries on the client's list that did not match the encrypted entries on the do not contact list.

Applicant respectfully submits that the combination of Morkel and Livingston does not describe the required limitations in amended claim 67. The proposed combination of Morkel and Livingston would have the "do not email" list of Livingston incorporated into the secure transmission of personal contact information of Morkel. However, as previously described, Morkel uses hashing to confirm the identity of the parties, and once the identity is

confirmed, unhashed data (personal contact information) will be shared. Personal contact information includes an email address (Col 1, lines 30-35). Thus, Morkel shares the underlying email address. Applicant's claimed invention, however, compares an encrypted email address on a client's list to encrypted email address on a do-not-contact list, "wherein the results of the comparison are an indication of which encrypted entries on the client's list match the encrypted entries on the do not contact list, and the results are not unencrypted entries of the do not contact list". Furthermore, Applicant's claimed invention also requires "transmitting at least an email to the email addresses in the client's list that correspond to the encrypted entries on the client's list that did not match the encrypted entries on the do not contact list".

As recognized by Livingston ("a do-not email list would well; unfortunately, such list could be seriously abused", Paragraph 4), by way of example and not limitation, Applicant's claimed invention allows a client email marketer the ability to identify email addresses on a do-not-contact list that are in the client's list without revealing the unhashed email addresses on the do-not-contact list or the client's list. Thus, by way of example and not limitation, Applicant's claimed invention prevents the abuse of the do-not-email list that is recognized by Livingston.

To illustrate, an email marketer has one list of email addresses that the email marketer wants to contact for marketing purposes and another party, in our example the government, has their own list of email addresses that make up a do-not-contact list. The email marketer is not allowed to contact email

addresses that choose to opt out of email marketing (i.e., the email addresses on the government's list) so the email marketer desires to check the entries on the government's list to determine if the email marketer should remove an entry from their list.

However, the government does not want to share their list of unhashed email addresses that do not wish to be contacted as this information can be very valuable to unscrupulous email marketers (e.g., if the list of unhashed email addresses were compromised then unscrupulous email marketers could contact the email addresses of people that do not wish to be contacted). Additionally, the email marketer also does not want to share their list of unhashed email addresses because this information is also very valuable to the email marketer and they do not want this list to be public for fear of unscrupulous email marketers (e.g., for the same reasons as above). Therefore, in Applicants' claimed invention a one-way hashing scheme is used by both entities (government and email marketer) such that each entity will have a list containing hashed entries. These two lists can then be compared and matches determined. Thus, with Applicants' claimed invention, for example, the content of the lists (i.e., the email addresses that on both lists) can be compared (e.g., by comparing the hashed entries on both lists) in order to modify the email marketer's list by removing the email addresses that appear on the government's do not email list without sharing the lists of unhashed email addresses. The email marketer may then transmit email messages to the email addresses that are not on their list that are not on the governments list.

Applicant respectfully submits that the dependant claims 68-70 depend on amended claim 67 and are allowable for at least the same reason.

Claim 71

Applicant respectfully submits that amended claim 71 includes similar limitations as in amended claim 67 with the addition that "the encrypted entries of the do -not-contact list were formed by encrypting information, including at least an email address that belongs to a minor" (Amended claim 71, emphasis added).

Applicant respectfully submits that the combination of Morkel and Livingston does not describe the required limitations in amended claim 71 for at least the same reasons as amended claim 67.

Applicant respectfully submits that the dependant claims 72-78 depend on amended claim 71 and are allowable for at least the same reason.

Claim 79

Amended claim 79 requires (emphasis added):

A computer implemented method to identify email addresses registered on a do-not-contact list without revealing the email addresses on the do-not-contact list comprising:

a client encrypting at least certain of entries on the client's list to create a plurality of encrypted entries, where each encrypted entry includes at least an email address that does not wish to be contacted, wherein the entries are

encrypted in a way that it is intended that an intended recipient cannot decrypt the entries;

the client causing a comparison of said plurality of encrypted entries from the client's list to a plurality of encrypted entries of a master do-not-contact list, wherein the encrypted entries of the master do-not-contact list were formed by encrypting information, including at least an email address that belongs to a minor, a matching of an encrypted entry from said plurality of encrypted entries from the client's list to an entry of the master do-not-contact list represents that the underlying email address needs to be identified;

the client receiving results of the comparison, wherein the results indicate at least one of the entries on the client's list is not on the master do-not-contact list, and the results do not reveal the email addresses on the master do-not-contact list; ~~and~~

the client updating the client's list with the results to remove the at least one of the entries on the client's list that is not on the master do-not-contact list.

the client transmitting at least an email to the at least one email address that corresponds to the removed entry.

Applicant respectfully submits that the combination of Morkel and Livingston does not describe the required limitations in amended claim 79. As previously described, the proposed combination of Morkel and Livingston would have the "do not email" list of Livingston incorporated into the secure transmission of personal contact information of Morkel. As previously described, Morkel uses hashing to confirm the identity of the parties, and once the identity is confirmed, unhashed data (personal contact information) will be shared. Personal contact information includes an email address (Col 1, lines 30-35). Thus, once the hashes match, personal contact information will be shared.

Applicant's claimed invention, however, requires identifying "email addresses registered on a do-not-contact list without revealing the email addresses on the do-not-contact list", and once a comparison is made, "the client receiving results

of the comparison, wherein the results indicate at least one of the entries on the client's list is not on the master do-not contact list, and the results do not reveal the email addresses on the master do-not-contact list", and the "client updating the client's list with the results to remove the at least one of the entries on the client's list that is not on the master do-not-contact list" and "the client transmitting at least an email to the at least one email address that corresponds to the removed entry" (amended claim 79).

Applicant respectfully submits that the dependant claims 80-82 depend on amended claim 79 and are allowable for at least the same reason.

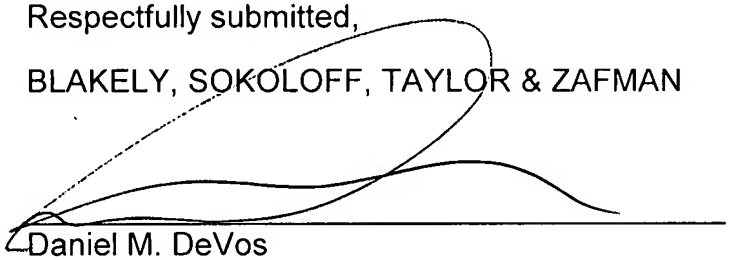
## CONCLUSION

Applicant respectfully submits that all rejections have been overcome and that all pending claims are in condition for allowance. If there are any additional charges, please charge them to our Deposit Account Number 02-2666. If a telephone conference would facilitate the prosecution of this application, Examiner is invited to contact Daniel M. DeVos at (408) 720-8300.

Respectfully submitted,

BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN

Date: October 25, 2007



Daniel M. DeVos
Reg. No. 37,813

1279 Oakmead Parkway
Sunnyvale, CA 94085-4040
(408) 720-8300